8-Port Gigabit managed POE Switch

User's Manual

Version: 2.3

September 9, 2007

TABLE OF CONTENT

1.0 INTRODUCTION 3
1.1 MAIN FEATURES 3
1.2 START TO MANAGE THIS SWITCH 5
2.0 WEB MANAGEMENT 6
2.1 CONFIGURATIONS 7
2.1.1.1 SYSTEM INFORMATION 7
2.1.1.2 DHCP 8
2.1.1.3 RELOCATE HTTP PORT NUMBER 8
2.1.1.4 TAG VLAN MANAGEMENT GROUP (CPU PORT) 8
2.1.2 PORTS 9
2.1.3 PORT-BASED VLAN 11
2.1.4 TAG-BASED VLAN 13
2.1.5 PORT TRUNKING 15
2.1.6 PORT MIRRORING 17
2.1.7 QUALITY OF SERVICE 19
2.1.8 STORM CONTROL 20
2.1.9 LACP 21
2.1.10 RSTP 23
2.1.11 IGMP 25
2.1.12 802.1X 26
2.1.13 POE STATUS AND COMMAND OPERATION 27
2.2 MONITORING 28
2.2.1. PORT STATISTICS 28
2.2.2 DETAILED PORT STATISTIC 29
2.2.3 LACP STATUS 30
2.2.4 RSTP STATUS 31
2.2.5 IGMP STATUS 32
2.2.5 PING 32
2.3 MAINTENANCE 33
2.3.1 WARM REBOOT 33
2.3.2 FACTORY DEFAULT 34
2.3.3 FIRMWARE UPDATE 34
2.3.4 CONFIG FILE 34
3.0 TERMINAL MODE MANAGEMENT 35

1.0 Introduction

8G web smart switch is a high performance web-smart switch that provides up to 8 10/100/1000Mbps copper Ethernet ports, this device provides a great flexibility for nowadays variety of network application but at lower cost. User doesn't have to learn many sophisticated management function which are usually shown in SNMP switch but just to learn some simple or common control or setting function through either out-of-band RS232 port or Ethernet port, however, some new, advanced and important function such as Tag-VLAN, Trunking, RSTP and IGMP are also supported same as SNMP switch, this means, user doesn't have to pay high cost as tradition layer 2 SNMP switch does while he still can get advanced or common function to meet requirement of general network application. This makes it very suitable for small or medium size company to build up simple network at beginning phase with lower cost. Besides, a optional long-ear accessory also makes it possible to operate in the rack mount environment.

Non-blocking and maximum wire speed performance are designed on all switched ports, it not only supports auto-negotiation but also AUTO-MDIX function on all switched 8 10/100/1000M RJ-45 Gigabit copper ports no matter running with half or full duplex mode, these function make user easy to use and reduce the matching effort between straight and cross-over line issues.

8G web smart switch supports both port-based and 802.1Q (tag-based) VLAN to catch-up the application needed in incoming VLAN age. To increase bandwidth application, it supports up to 4 trunk groups with maximum 8 ports on one Trunk, moreover, these trunk ports are with fair-over function to provide redundant back-up when one or some of trunk ports malfunction. Moreover, to reduced convergent time of STP protocol, Rapid STP (RSTP) is supported, to support multicast application IGMP is also supported. ,

Fully LED status display ease user's installation, a reset button is also provided to make user easy to go back to default setting.

1.1 Main Features

This switch provides the following main features:

- Non-blocking, full-line speed, store-and-forward
- Support jumbo frame, Max. packet length 9600 bytes
- Auto-Negotiation and Auto-MDIX on all 10/100/1000M copper ports
- Up to 8 10/100/1000 RJ-45 copper ports
- 144K byte packet buffer, 8K MAC entries
- Support port-based VLAN and tag-based (802.1Q) VLAN
- Support RSTP, IGMP, DHCP

- Support “relocate port number” to “ http operation “
- Port trunk with fail-over capability
- Support flow control for both full/half duplex operations
- Support Multicast storm, Broadcast Storm control as well as Flooding Control
- Support port mirroring
- LED display for each port to show link and activity status
- Desktop and optional Rack mountable kit
- Reset to default “ push button “ and field code upgradeable

1.2 Start to Manage This Switch

Either way user may start to manage this switch, web mode through Ethernet port or terminal mode through RS232 port.

1,2,1 Web mode default setting are:

Default IP Address: 192.168.223.100
Default IP mask: 255.255.255.0
Default gateway: 192.168.223.254
Default Password (blank), press “enter” key in the password field

1.2.2 Terminal mode default setting are: baud rate: 115,200, attribute: 8, None, 1, None
Terminal mode operation: (no password is needed)

Once terminal is connected, the basic operation rule are shown below

Press “ ? “ to find root operation page, then choose command by typing little alphabets

After enter command page, Press “ ? “ to find command parameters and format,
further more, type “ command ? “ to get explanation.

Type “ up “ or “ / “ to go back to previous page

2.0 Web management

After login is successfully validated, the switch's home page will show up. The left part on the page provides the *function menus*, while the right part provides the individual configuration value or system parameters value. Function manus are divided into three categories, they are **Configuration, Monitoring and Maintenance,** all functions are shown briefly below

Configuration

- **System** – system values, such as H/W, F/W version, IP, IP mask, MAC address…etc
- **Ports** – port status and configure port parameters
- **Port-based VLAN** – to setup the port-based VLAN
- **Tag-based VLAN** – to configure the tag-based VLAN
- **Port Trunking** – to build up the trunk function
- **Port Mirroring** – to setup the port mirroring function
- **Quality of Service** – to configure the Quality of Service function
- **Storm Control** – to set all kinds of storm limit
- **LACP** – to set LACP parameter
- **RSTP** – to set RSTP parameter
- **IGMP** – to set IGMP parameter
- **802.1X** – to set 802.1X parameter

Monitoring:

- **Port Statistics** – to statistic traffic on each ports
- **Detailed Port Statistics** – to statistic more detailed traffic on each ports
- **LACP status** – to show LACP status
- **RSTP status** – to show RSTP status
- **IGMP status** – to show IGMP status
- **Reset** – to reboot the switch with/without writing default configurations
- **Ping** – provide ping function and ping result

Maintenance

- **Warm Reboot** – to restart system
- **Factory Default** – to get parameter value back to factory default
- **Firm Upgrade** – to upgrade code
- **Config File** – to backup configuration data
- **Logout – to logout**

2.1 Configurations

2.1.1.1 System information

The system diagram shows every common system information, they are H/W, F/W version, MAC address, IP address, subnet mask, IP gateway, default VLAN value of management port, name, password, timeout value, and SNMP communities…etc. Once user finish the setting, he must press the " Apply " button to execute all his setting, and whenever he needs, he may press the " Refresh " button to get updated status of system information.

System Configuration

Model Name	8G_PoE_Smart
MAC Address	00-0a-17-02-14-ec
F/W Version	2.0
H/W Version	1.0
DHCP Enabled	☐
IP Address	192.168.223.110
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
HTTP Listening Port Number	80 (1024 - 65535)
Tag VLAN Management Group	1
Name	
Password	
Inactivity Timeout (secs)	0
SNMP enabled	☑
SNMP Trap destination	0.0.0.0
SNMP Read Community	public
SNMP Write Community	private
SNMP Trap Community	public

Apply Refresh

2.1.1.2 DHCP

The default DHCP is off, so Default IP or user defined IP is used when this machine is turning-ON, but if this switch needs an IP assigned from DHCP server, user may click the square field and then press " Apply " to get an IP which will be assigned by DCHP server ". User must be aware that if he enable DHCP from web page, and if the DHCP server is working, then after enable DHCP, he will lose contact of web page, because the IP address has been changed.

2.1.1.3 relocate HTTP port number

The default port number of **HTTP command** is 80, but unauthorized user may intrude this switch if he knows the IP of this switch, network manager may relocate this port number to other value, from 1024 to 65535, the same idea as above, once network manager change the value of HTTP's port number, he will lost contact and he must regain web page by command modified as below:

http://192.168.223.100:port_value

2.1.1.4 Tag VLAN management group (CPU port)

At first time you turn on this device, all ports belong to default VLAN ID group (VID=1), so they can communicate to each other, and hence any port can be used as web management port to talk with CPU port inside, but, for example, assume user uses port 1 as web management port, then user create VLAN ID=10 on port 7,8 and create another VLAN ID = 20 on port 5,6, now 3 VLAN groups will be shown on VALN group table after he press " Apply " button. Meanwhile, Tag VALN management Group on System page now will be shown 3 options to select, **user may assign CPU port to one of VLAN groups by press „Apply" command, so that he can continue configure or manage switch through any one port of selected VLAN group.** . If VLAN 10 and VLAN ID 20 must be isolated, then user must delete original member port 5,6,7,8 in default VLAN group (VID = 1). And if user forget what group that CPU belongs to, there are two ways to solve this condition below.

(1) Through console port, change VLAN ID of CPU port under IP Setup command if he gets password, or
(2) Press **"Reset"** button **few seconds**, let system return to default settings, that is,
---- >> IP address=192.168.223.100; … VID=1, and all settings return to factory default

2.1.2 Ports

Port status page always shows current port status of all 8 ports. User can set link mode, enable or disable flow control and jumbo frame, however, be noticed that the jumbo frame is global setting, it can't be set on individual port but on all ports at a time. A default diagram is shown below,

Port Configuration

Port	Link Status	Link Mode	Flow Control
1	100FDX	Auto Speed	☐
2	Down	Auto Speed	☐
3	Down	Auto Speed	☐
4	Down	Auto Speed	☐
5	Down	Auto Speed	☐
6	Down	Auto Speed	☐
7	Down	Auto Speed	☐
8	Down	Auto Speed	☐

Enable Jumbo Frames ☐

Apply Refresh

Choose and click the ports you want to set, for example, choose port 1, and set port 1 Flow Control enable, then press "Apply", after execution, diagram will shown below

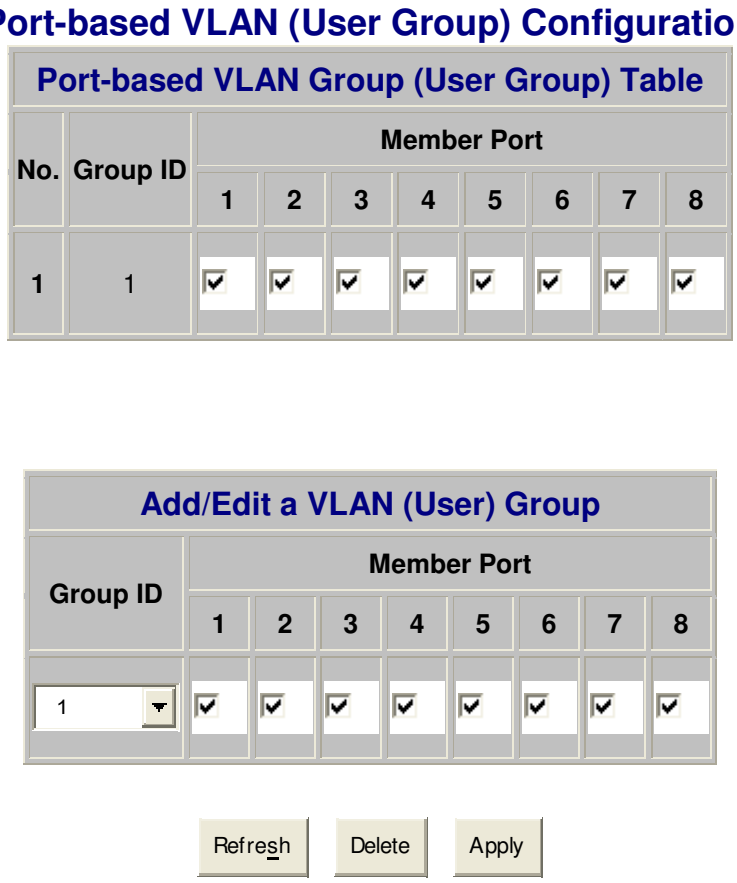
Port Configuration

Port	Link Status	Link Mode	Flow Control

1	100FDX	Auto Speed	☑
2	Down	Auto Speed	☐
3	Down	Auto Speed	☐
4	Down	Auto Speed	☐
5	Down	Auto Speed	☐
6	Down	Auto Speed	☐
7	Down	Auto Speed	☐
8	Down	Auto Speed	☐

2.1.3 Port-based VLAN

Port-based VLAN is a kind of VLAN which is a group of ports marked as a kind by group ID, different VLAN (different ID) can't communicate to each other. Before the setting, user must be aware of that there is a default Port-based VLAN, his group ID is 1, so, if user wants to set another new port-based VLAN, better set another group ID rather than 1. After press " Apply " button, the screen will show a new port-based VLAN if he add a new group or screen will delete a port-based VLAN if he delete a group. The important thing is that port-based VLAN is valid only within same device, it will never be valid cross the devices. A default diagram is shown below.



Choose and click the ports you want to group, for example, choose port 1, port 2 and set their group ID 2, then press "Apply", after execution, diagram will shown below

Port-based VLAN (User Group) Configuration

Port-based VLAN Group (User Group) Table

No.	Group ID	Member Port							
		1	2	3	4	5	6	7	8
1	1	☑	☑	☑	☑	☑	☑	☑	☑
2	2	☑	☑	☐	☐	☐	☐	☐	☐

Add/Edit a VLAN (User) Group

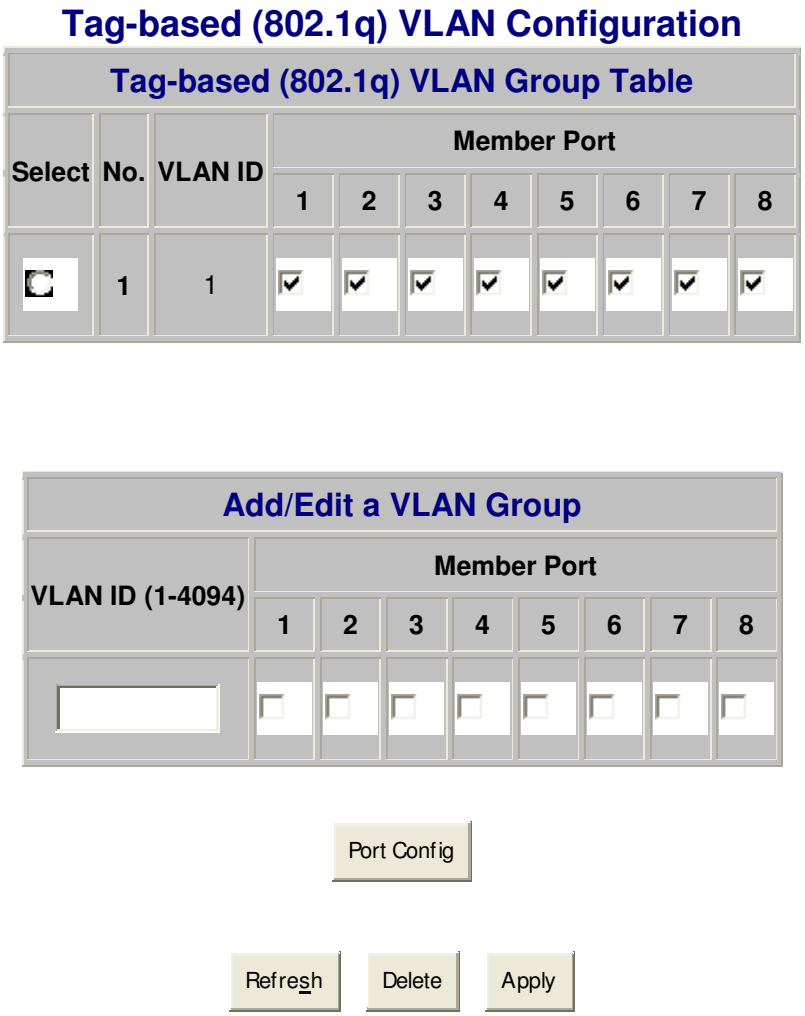
Group ID	Member Port							
	1	2	3	4	5	6	7	8
2	☑	☑	☐	☐	☐	☐	☐	☐

Refresh Delete Apply

2.1.4 Tag-based VLAN

Tag-based VLAN is another kind of VLAN which is a group of ports marked as same kind by assigning a tag-value on each port, same as port-based VLAN, different VLAN (different ID) can't communicate to each other, and before the setting, there is a default tag-based VLAN, which ID is 1 (VLAN ID=1), so, if he wants to set another new tag-based VLAN, better set another VLAN ID rather than 1 (tag-base VALN ID ranged from 1 ~ 4094). After press " Apply " button, the screen will show a new tag-based VLAN if user add a new VALN, or, a tag-VLAN will be vanished if user delete a VLAN. Two important things must be emphasized here, one is that tag-based VLAN members are valid not only within same device, but also cross the devices as long as they are with same VLAN ID; the other important thing is user must keep in mind that the management-port (CPU port)VLAN ID should be the same as some member VLAN ID if user want to management through that port, or, management communication will be failed because different VLAN (different ID) can't communicate to each other.

A default diagram is shown below.



After assign a tag VLAN, there are further attributes parameter can be assigned for some advanced tag-VLAN application, here below are explanation when entering the " Port Config ", they are:

1. VLAN Aware mode:
   Enable - Strip VLAN tag from received frame, and insert VLAN tag in transmitted frame except ingress frames which tag VID = PVID
   Disable – default state, this means, switch doesn't do VLAN tag stripping and insertion.

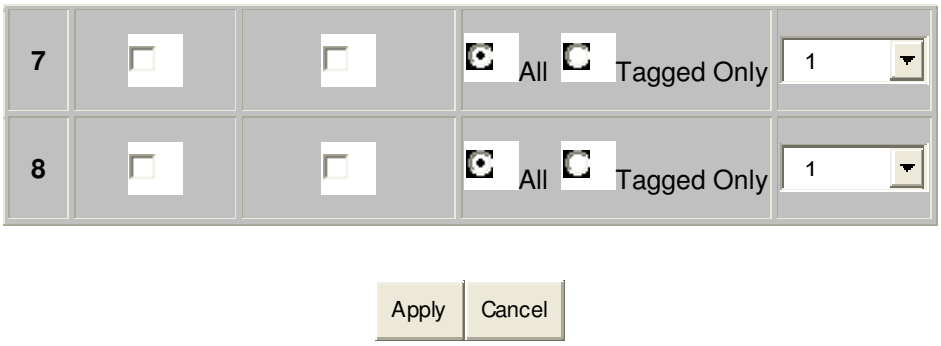
2. Ingress filtering:
   Enable - Check ingress frame VLAN ID. Ingress frame will be dropped if frame's VID is not the same as the VID of the ingress port which belongs to a member of a VLAN group
   Disable – Don't do ingress VLAN frame checking, the frame will be flood if VID is not the same

3. Accept Packet Type:
   ALL - Accept all ingress frames
   Tagged only - Only accept ingress frames with VLAN tag

4. Port VID:
   Set port VLAN ID for untagged ingress frames. Set "None" for trunk port member.

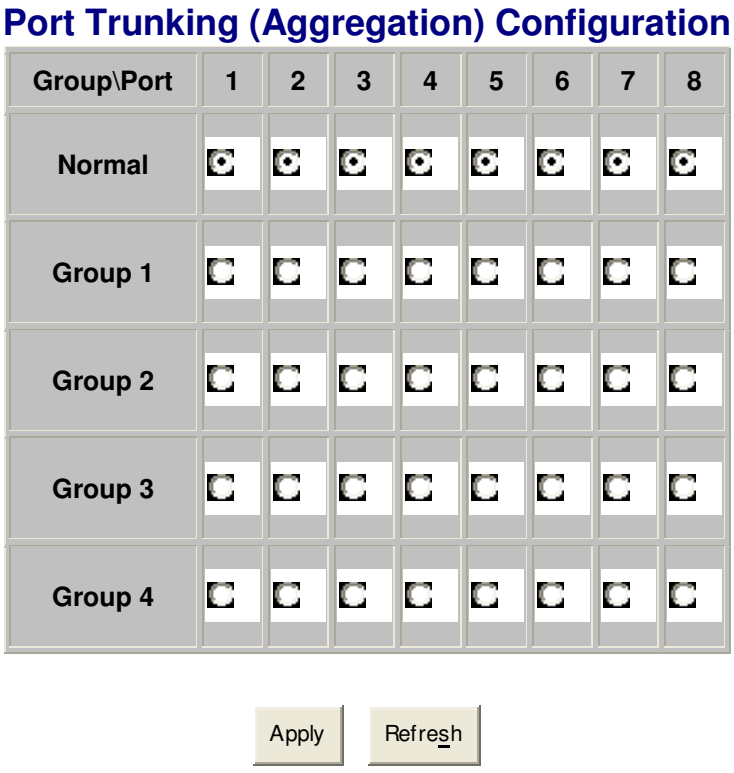
Tag VLAN Per Port Configuration

Port	VLAN aware Enabled	Ingress Filtering Enabled	Acceptable Packet Type	Port VID
1	☐	☐	◉ All ○ Tagged Only	1
2	☐	☐	◉ All ○ Tagged Only	1
3	☐	☐	◉ All ○ Tagged Only	1
4	☐	☐	◉ All ○ Tagged Only	1
5	☐	☐	◉ All ○ Tagged Only	1
6	☐	☐	◉ All ○ Tagged Only	1

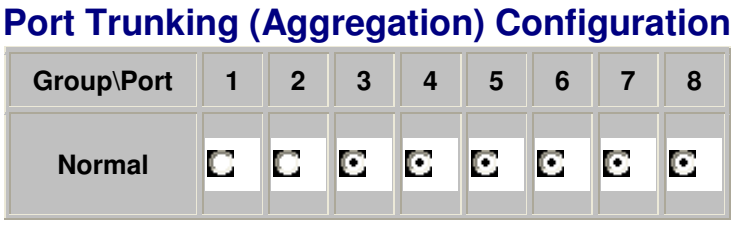


2.1.5 Port Trunking

A default diagram is shown below, and up to 4 groups are provided



Choose and click the trunk ports you want to group, for example, choose port 1, port 2 into group 1, then press “Apply”, after execution, diagram will shown below

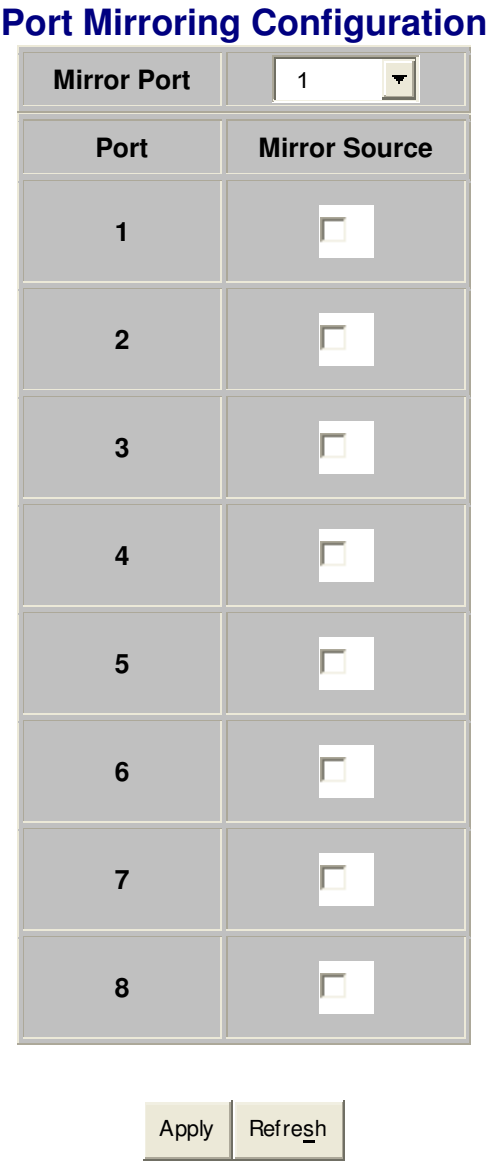


Group 1	◉	◉	○	○	○	○	○	○
Group 2	○	○	○	○	○	○	○	○
Group 3	○	○	○	○	○	○	○	○
Group 4	○	○	○	○	○	○	○	○

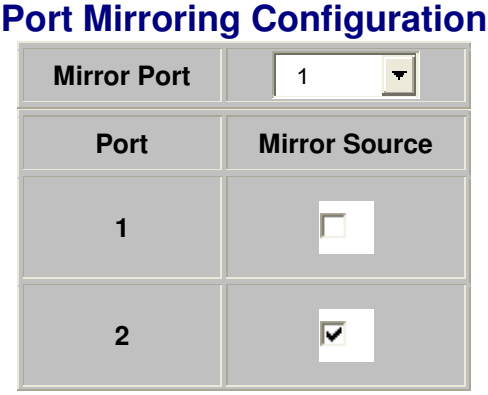
Apply Refresh

2.1.6 Port Mirroring

A default diagram is shown below,



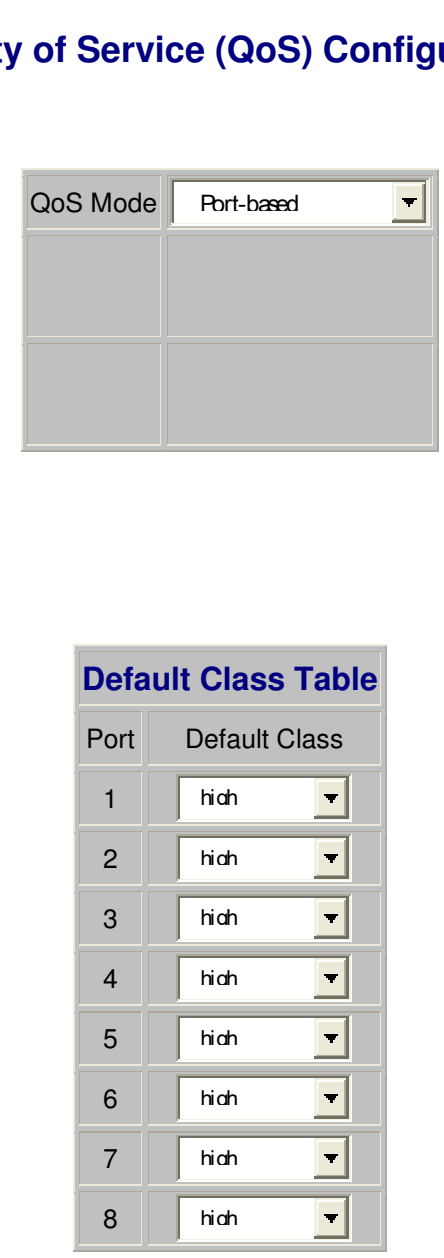
Choose and click the ports you want to monitor, for example, choose port 2
To be monitored, then press “Apply”, after execution, diagram will shown below



3	
4	
5	
6	
7	
8	

2.1.7 Quality of Service

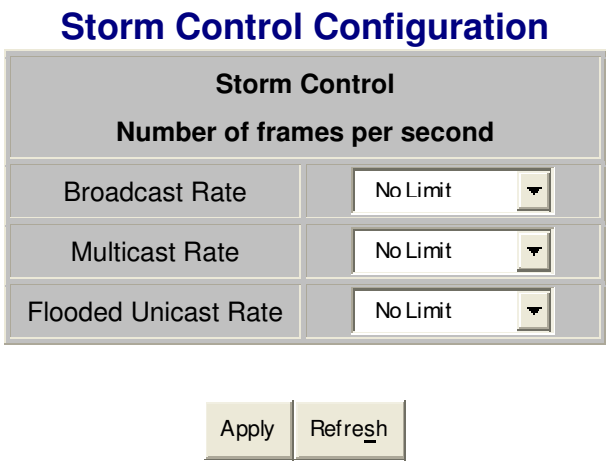
A default diagram is shown below,



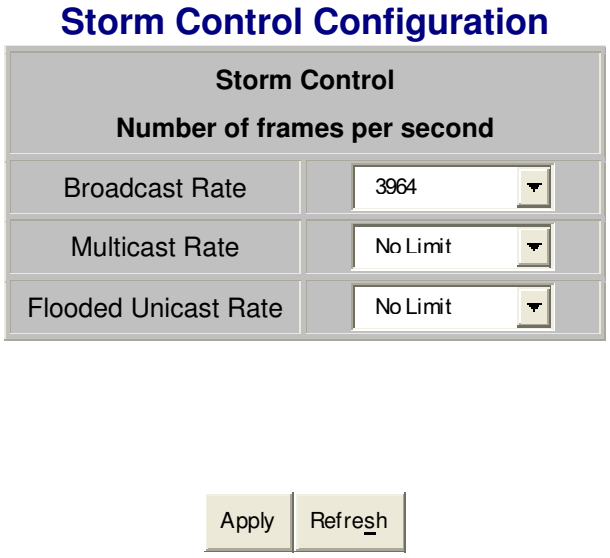
Choose the priority level for the port you want to set, then same priority will get same priority service.

2.1.8 Storm Control

A default diagram is shown below,

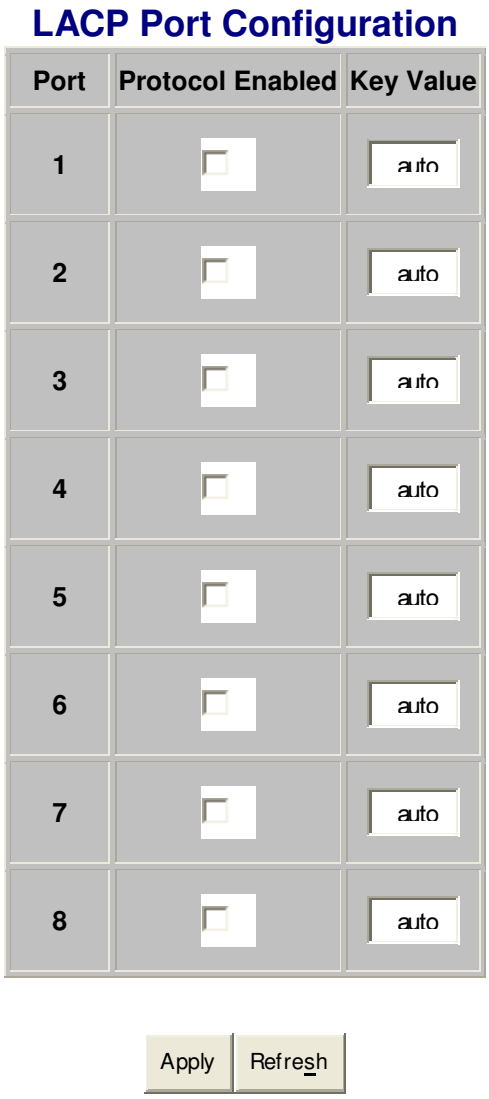


Choose and click type of storm you want to control, for example, choose Broadcast storm with 3,964 frames per second as upper limit, once the Broadcast frame rate higher than 3,964 frame per second, this port will be disabled. Press “Apply”, after execution, diagram will be shown below



2.1.9 LACP

Different from the static port trunking, LACP provides another way to dynamically aggregate port to a group (trunk) according to IEEE 802.3ad. A default diagram is shown below,



Two parameters need to be set per port basis in this webpage:

- **Protocol Enabled** – to enable/disable LACP protocol for a port.
- **Key Value** – a number (1~255) to identify the LACP group for a port. All member ports in a LACP group have the same key values. Key number will be automatically generated if "auto" value is set

Choose and click the trunk ports you want to group. For example, select port 7 and port 8 to group into a LACP group with key value 20 for both ports, then press " Apply" to activate the setting. The following figure is the result:

LACP Port Configuration

Port	Protocol Enabled	Key Value
1	☐	auto
2	☐	auto
3	☐	auto
4	☐	auto
5	☐	auto
6	☐	auto
7	☑	20
8	☑	20

Apply Refresh

2.1.10 RSTP

The Spanning-Tree Protocol (STP) is IEEE 802.1d standardized method for avoiding loops in switched networks. Enable STP to ensure that only one path at a time is active between any two nodes on the network.

The Rapid-Spanning-Tree-Protocol (RSTP) is a more advanced protocol than STP according to IEEE 802.1w standard. RSTP can shorten spanning tree convergent time while network topology is changed. A default diagram is shown below,

RSTP Configuration

System Configuration	
System Priority	32768
Hello Time	2
Max Age	20
Forward Delay	15
Force version	Normal

Port Configuration			
Port	Protocol Enabled	Edge	Path Cost
Aggregations	☐		
1	☐	☑	auto
2	☐	☑	auto
3	☐	☑	auto
4	☐	☑	auto
5	☐	☑	auto

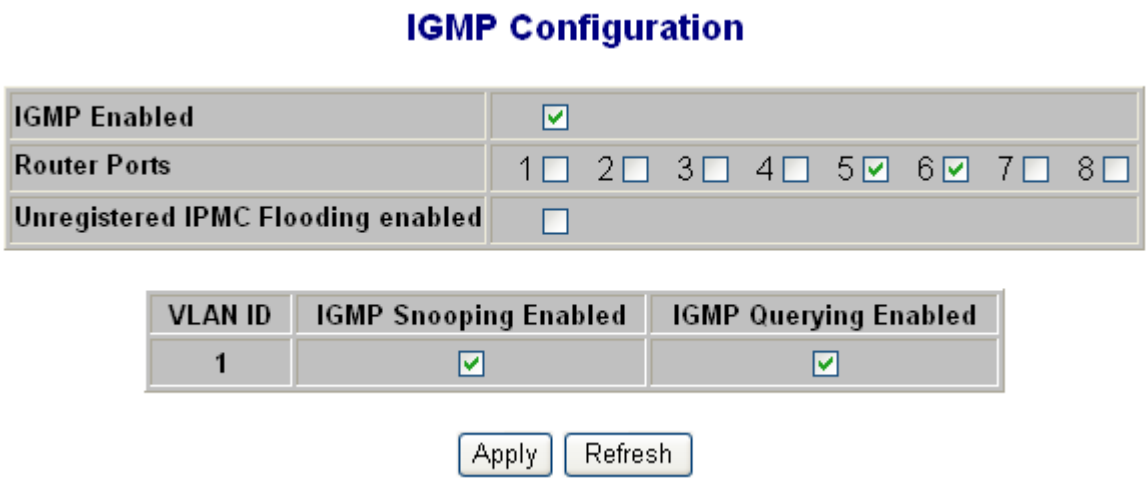
Use the following parameters in the webpage to configure RSTP function:

- **System Configuration**
  - **System Priority** – A value to identify the root bridge. The bridge with lowest value has the highest priority and is selected as the root. 16 numbers are provided in this field from 0 to 61140 in increments of 4096.
  - **Hello Time** -- the number of seconds among the transmission of Spanning-Tree Protocol configuration messages. Enter a number 1 through 10. (default is 2)
  - **Max Age** – the number of second bridge waits without receiving Spanning-Tree Protocol configuration messages before attempting a reconfiguration. Enter a number 6 through 40. (default is 20)
  - **Forward Delay --** the number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a number 4 through 30. (default is 15)
  - **Force Version** – normal: use RSTP; compatible: compatible with old STP protocol

- **Port Configuration**
  - **Aggregations** – Enable/disable the RSTP protocol on aggregation links
  - **Protocol Enabled** – Enable/disable the RSTP protocol per port basis
  - **Edge** – Enable/disable to expect a port to be an edge port (an end station) or a link to another STP device
  - **Path Cost** – A value on a port that switch uses to determine which port are the forwarding ports. The lowest number is forwarding ports. The value can be set from 1 to 200000000 or “auto” to be automatically generated.

2.1.11 IGMP

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IGMP can manage the multicast traffic if the members (switches, router or other network devices) of group support IGMP. This switch provides IGMP snooping feature to detect IGMP queries, report packets and manage the IP multicast traffic through the switch. This feature can limit the forwarding of multicast frames to only ports that are a member of multicast group. Only **IPv4** IGMP frames are recognized for this system.



The following parameters are provided for configuring IGMP snooping for this system:

- **IGMP Enabled** – to globally enable/disable IGMP snooping function
- **Router Ports** – to specify administrative router ports for IGMP frames
- **Unregistered IPMC Flooding Enabled** – to set forwarding option for unregistered (not joined) IP multicast traffic. Enabled: to flood frames; Disable: to forward frames to **router ports** only

Two options can be set for each existing VLAN group:

- **IGMP Snooping Enabled** – to enable/disable snooping IGMP frames
- **IGMP Querying Enabled** – to enable/disable sending IGMP querying frames

The example webpage show in above shows the configuration of IGMP function which has IGMP enabled, uses port 5 and 6 as router ports to forward the IGMP frames, forwards unregistered IPMC frames to router ports (port 5 and 6), and enables snooping IGMP and sending querying frames for the VLAN group which VID = 1.

2.1.12 802.1x

A default diagram is shown below, user must contact the manager of RADIUS server, and then get IP, UDP port number and secret to operate 802.1X.

802.1X Configuration

Mode	Disabled
RADIUS IP	0.0.0.0
RADIUS UDP Port	1812
RADIUS Secret	

Port	Admin Mode	Port State	Action		
1	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
2	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
3	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
4	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
5	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
6	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
7	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
8	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
			Re-authenticate All	Force Reinitialize All	

Apply Refresh

2.1.13 PoE status and command operation

Some status definition described below before you read or execute the command,

Non-PD, this means there is an ethernet device but not PD device is loaded
No Load: there is not any PD device being loaded to that port, but non-PD may be
Loaded: a PD device is being loaded, class level and allocated power is shown
PD Error: over current event (exceed 350 ma) happened, and port is disabled automatically
Dedicated class, display the class level of current loaded PD device
Allocated power, maximum allocated power to that port , but not current power

PoE Port Configuration

Port	PSE Power	Detected Class	Allocated Power	PoE Status
1	Enable	3	15 W	Loaded
2	Enable	N/A	0 W	No Load
3	Disable	3	0 W	PD Error
4	Enable	N/A	0 W	No Load
5	Enable	N/A	0 W	No Load
6	Enable	N/A	0 W	No Load
7	Enable	N/A	0 W	No Load
8	Enable	N/A	0 W	Non-PD

System Max. Supplied Power (A)	**120 Watt**
Total Allocated Power (B)	**15 Watt**
Power Balance (C = A - B)	**105 Watt**

Apply Refresh

IEEE 802.3af Class - Power Table

IEEE 802.3af Class	0	1	2	3	4
PSE Output Power	15W	4W	7W	15W	Reserved

2.2 Monitoring

2.2.1. Port Statistics

Choose and click command manual, after execution, diagram will shown below, user can clear counter or refresh as will

Statistics Overview for all ports

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	0	0	0	0	0	0
2	4837	7	1122	9	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0

Clear Refresh

2.2.2 Detailed Port Statistic

Choose and click command manual, more detailed count will be displayed like below, user can analyze frame per frame size, byte and error types.

Statistics for Port 2

Clear | Refresh

Port 1 | Port 2 | Port 3 | Port 4 | Port 5 | Port 6 | Port 7 | Port 8

Receive Total		Transmit Total	
Rx Packets	152	Tx Packets	32
Rx Octets	12525	Tx Octets	19735
Rx High Priority Packets	-	Tx High Priority Packets	-
Rx Low Priority Packets	-	Tx Low Priority Packets	-
Rx Broadcast	-	Tx Broadcast	-
Rx Multicast	-	Tx Multicast	-
Rx Broad- and Multicast	112	Tx Broad- and Multicast	0
Rx Error Packets	0	Tx Error Packets	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	-	Tx 64 Bytes	-
Rx 65-127 Bytes	-	Tx 65-127 Bytes	-
Rx 128-255 Bytes	-	Tx 128-255 Bytes	-
Rx 256-511 Bytes	-	Tx 256-511 Bytes	-
Rx 512-1023 Bytes	-	Tx 512-1023 Bytes	-
Rx 1024- Bytes	-	Tx 1024- Bytes	-
Receive Error Counters		**Transmit Error Counters**	
Rx CRC/Alignment	-	Tx Collisions	-
Rx Undersize	-	Tx Drops	-
Rx Oversize	-	Tx Overflow	-
Rx Fragments	-		
Rx Jabber	-		
Rx Drops	-		

2.2.3 LACP Status

Choose and click command manual, after execution, diagram will shown like below, user can refresh as will

LACP Status

LACP Aggregation Overview</FONT< th>								
Group/Port	1	2	3	4	5	6	7	8
State								

Legend		
	Down	Port link down
0	Blocked	Port Blocked by RSTP. Number is Partner port number if other switch has LACP enabled
0	Learning	Port Learning by RSTP
	Forwarding	Port link up and forwarding frames
0	Forwarding	Port link up and forwarding by RSTP. Number is Partner port number if other switch has LACP enabled

Refresh

LACP Port Status			
Port	Protocol Active	Partner Port Number	Operational Port Key
1	no		
2	no		
3	no		
4	no		

5	no		
6	no		
7	no		
8	no		

2.2.4 RSTP Status

Choose and click command manual, after execution, diagram will shown like below, user can refresh as will

RSTP Status

RSTP VLAN Bridge Overview						
VLAN Id	**Bridge Id**	**Hello Time**	**Max Age**	**Fwd Delay**	**Topology**	**Root Id**
1	32769:00-01-c1-00-00-02	2	20	15	Steady	This switch is Root!

Refresh

RSTP Port Status						
Port/Group	**Vlan Id**	**Path Cost**	**Edge Port**	**P2p Port**	**Protocol**	**Port State**
Port 1						Non-STP
Port 2						Non-STP
Port 3						Non-STP
Port 4						Non-STP
Port 5						Non-STP
Port 6						Non-STP
Port 7						Non-STP
Port 8						Non-STP

2.2.5 IGMP Status

Choose and click command manual, after execution, diagram will shown like below, user can refresh as will

IGMP Status

VLAN ID	Querier	Queries transmitted	Queries received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
1	Idle	0	0	0	0	0	0

Refresh

2.2.5 Ping

A default diagram is shown below,

Ping Function

Ping parameters	
Target IP address	
Count	1
Time Out (in secs)	1

Apply

Ping Results	
Target IP address	0.0.0.0
Status	Test complete
Received replies	0
Request timeouts	0

Average Response Time (in ms)	0

Refresh

Fill up the IP address you want to ping, set Time Out time and Counts, for example,
IP = 192.168.223.254, count = 5, time pout = 5 sec, then press “Apply”, then press “Refresh” after execution, diagram will shown below

Ping Results	
Target IP address	192.168.223.254
Status	Test complete
Received replies	0
Request timeouts	5
Average Response Time (in ms)	0

Refresh

2.3 Maintenance

2.3.1 Warm Reboot

Choose and click command manual, diagram will shown like below, user can press Yes or No

Warm Reboot

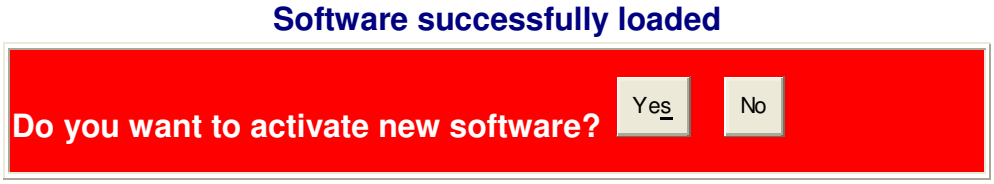
Are you sure you want to perform a warm reboot? Yes No

2.3.2 Factory Default

Choose and click command manual, diagram will shown like below, user can press Yes or No

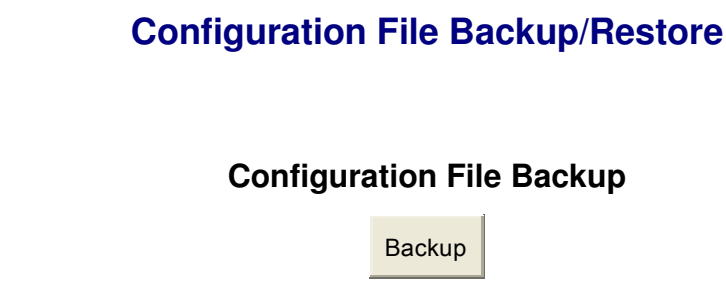
2.3.3 Firmware Update

Choose and click command manual, diagram will be shown, and then direct the location of the file that to be updated, then press " upload ", if success, it will be shown below



2.3.4 Config File

Choose and click command manual, diagram will be shown, and then direct the location of the file that to be backup, give a name, then press " Backup "



Choose and click command manual, diagram will be shown, and then direct the location of the file that to be restored, then press " Restore " It will show transfer completed if it success.

Configuration File Restore

Restore

3.0 Terminal Mode management

Terminal mode is easy to operate, it is useful when in-band ethernet communication is malfunction, or user wants to do some parameter setting, for example, before in-band management through ethernet works, user might have to modify IP address, subnet mask, …etc, he may do these things through terminal mode.

No password is needed in terminal mode operation, but before it starts, user must set up the terminal parameters, such as Hyper terminal in Microsoft Window,

Select COM #: COM 1, COM 2, …then,
Set Baud rate to: 115,200, per second
Set Attribute to 8, None, 1, None (8 bit, No parity, 1 stop bit, No protocol in hardware)

Once terminal is connected, the basic operation rule are shown below

Press " ? " to find root operation page, then choose command by typing little alphabets
The screen will show as below

```
>?
Commands at top level:
System          - System commands
Console         - Console commands
Port            - Port commands
MAC               - MAC commands
VLAN              - 802.1q (Tag-based) VLAN commands
Aggr            - Aggregation commands
LACP              - IEEE 802.3ad Link Aggregation commands
RSTP              - IEEE 802.1w Rapid Spanning Tree commands
User Group    - User Group (Port-based VLAN) commands
QoS               - QoS commands
Mirror          - Mirror commands
IP              - IP commands
Dot1x           - Dot1x commands
IGMP              - IGMP Snooping commands
Debug           - Debug commands
```

>

After enter command page, Press " ? " to find command parameters and format, for example

>system
System>

System>?
Commands at System level:
System Configuration [all]
System Restore Default [keep IP]
System Name [<name>]
System Reboot
System Xmodem
System SNMP [enable|disable]
System Trap [<IP Address>]
System Read community [<community string>]
System Write community [<community string>]
System Trap community [<community string>]

further more, type " command " to get more information, such as type "configuration"

System>configuration
System Configuration:
    Name:
    S/W Version: 1.1
    CVS Tag: sw_8051_2_29e
    Compile Date: Dec 18 2006 12:26:43
    H/W Version: 1.0

    MAC address: 00-0a-17-02-10-06
    SNMP: enabled
    Trap IP: 0.0.0.0
    Read community: public
    Write community: private
    Trap community: public

Type " up " or " / " go back to previous page

All others command are operated likewise.